Exhibit A

Click here to Respond to Selected Documents

Sort Date Entries: Descending Ascending

Display Options: All Entries

05/29/2025

Corporation Served
Document ID - 25-SMCC-3008; Served To - AMERICAN MULTISPECIALTY GROUP INC; Server - ; Served Date - 28-MAY-25; Served Time - 00:00:00; Service Type - Special Process Server; Reason Description - Served

Notice of Service
Return of Service.
Filed By: JOHN FRANCIS GARVEY JR
On Behalf Of: MARY WIPPOLD

05/23/2025

Summons Issued-Circuit
Document ID: 25-SMCC-3008, for AMERICAN MULTISPECIALTY GROUP INC

05/20/2025

Filing Info Sheet eFiling

Filed By: JOHN FRANCIS GARVEY JR

Motion Special Process Server
Request for Appointment of Special Process Server.
Filed By: JOHN FRANCIS GARVEY JR

Pet Filed in Circuit Ct
Class Action Petition; Exhibit A; Exhibit B; Exhibit C.
Filed By: JOHN FRANCIS GARVEY JR

IN THE CIRCUIT COURT OF THE CITY OF ST. LOUIS
STATE OF MISSOURI

MARY WIPPOLD, individually and on behalf of all others similarly situated,	)	
Plaintiff,	)	
V.	)	**Case No. _____**
AMERICAN MULTISPECIALTY GROUP, INC., d/b/a ESSE HEALTH	)	JURY TRIAL DEMANDED
SERVE AT: 12655 OLIVE BOULEVARD FOURTH FLOOR ST. LOUIS, MISSOURI, 63141	)	
Defendant.	)	

CLASS ACTION PETITION

Plaintiff, MARY WIPPOLD, individually, and on behalf of all others similarly situated (hereinafter, "Plaintiff"), brings this Class Action Petition against Defendant, American Multispecialty Group, Inc., d/b/a Esse Health ("Esse," "Esse Health" or "Defendant"), and alleges upon personal knowledge as to her own actions, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. This action arises out of the public exposure of the confidential, private information of Esse's current and former patients—Plaintiff and the proposed Class Members—in late April 2025 during a cyberattack, caused by Defendant's failures to adequately safeguard that information ("the Data Breach"). On information and belief, the information impacted in the Data Breach

includes Personally Identifying Information[1] ("PII") and Protected Health Information ("PHI")[2] (collectively "Private Information").[3]

2. Headquartered in St. Louis, Missouri, Esse Health is a massive medical system, "with over 170 providers and 45 offices in and around the St. Louis Metropolitan area, Esse Health proudly remains at the forefront of compassionate and innovative healthcare."[4]

3. As a condition of receiving treatment and services from Esse, Defendant required its patients to provide it with their sensitive Private Information, which Esse promised to protect from unauthorized disclosure.

4. Defendant failed to undertake adequate measures to safeguard the Private Information of Plaintiff and the proposed Class Members, including failing to implement industry standards for data security, and failing to properly train employees on cybersecurity protocols, resulting in the Data Breach.

---

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8)..

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). Esse Health is clearly a "covered entity" and some of the data compromised in the Data Breach is "protected health information," subject to HIPAA.

[3] *See Network Update,* avail. at https://www.essehealth.com/network-updates/ (last accessed May 16, 2025), **attached as Exhibit A.**

[4] https://www.essehealth.com/about-us/our-story/ (last accessed May 16, 2025).

5. As a direct and proximate result of Defendant's failures to protect current and former patients' sensitive Private Information and warn them promptly and fully about the Data Breach, Plaintiff and the proposed Class Members have suffered widespread injury and damages, including interruption of care, necessitating Plaintiff to seek relief on a class wide basis.

PARTIES

6. Plaintiff is a natural person and resident and citizen of the State of Missouri, where she intends to remain, who resides in the City of St. Louis. Plaintiff is a current patient of Esse and a Data Breach victim.

7. Plaintiff resided in the City of St. Louis when her data was first breached in April 2025, causing her injury and damages, due to Defendant acts and omissions as set forth herein.

8. Defendant, Esse Health, is a privately held independent physician group formed under the laws of the State of Missouri with a principal place of business at 12655 Olive Boulevard, 4th Floor, St. Louis, Missouri, 63141, in St. Louis County.

9. Esse Health's Registered Agent for Service of Process is 12655 Olive Boulevard, 4th Floor, St. Louis, Missouri, 63141, in St. Louis County.

JURISDICTION & VENUE

10. This Court has subject-matter jurisdiction pursuant to Mo. Stat. § 478.070.

11. This Court has personal jurisdiction over Defendant because it maintains a principal place of business in Missouri, and provides healthcare and related services in Missouri.

12. Venue is proper in this Court pursuant to Mo. Stat. § 508.010 because Plaintiff was first injured by Defendant's acts and omissions in the City of St. Louis, Missouri where she resided at the time of the Data Breach, and as Defendant does business in the City of St. Louis, Missouri.

COMMON FACTUAL ALLEGATIONS

A. Defendant Collects and Promises to Protect Patient Private Information

13. Esse Health is a massive medical system, and "with over 170 providers and 45 offices in and around the St. Louis Metropolitan area, Esse Health proudly remains at the forefront of compassionate and innovative healthcare."[5]

14. According to Esse Health, the St. Louis Business Journal named Esse Health to the "2019 list of the Top 150+ Privately Held Companies in the area."[6] According to Esse Health, "[o]ut of the 200 companies recognized, Esse Health ranked 74th on the list with a total revenue of $345 million and a growth of 14.6% for 2018."[7]

15. As Esse Health states on its website:

> Esse Health is a St. Louis-based, independent physician group that strives to improve the overall well-being of its patients through patient education, lifestyle modification and prevention. Esse Health has been awarded Patient-Centered Medical Home (PCMH) 2017 recognition by the National Committee on Quality Assurance. The U.S. Department of Health and Human Services' Million Hearts Initiative recognized Esse Health as a 2014 Hypertension Control Champion for its success in helping patients control their high blood pressure. With 45 locations throughout the St. Louis and Metro East area, Esse Health's services include asthma, allergy and immunology, family medicine, gastroenterology, internal medicine, nutrition, orthopedics, pediatrics, radiology and urology. Esse Health is a recognized leader in using technology in health care and physician accountability for both quality and cost-of-care. [8]

16. As a condition of rendering medical and other treatment, Defendant requires that its patients provide Esse with massive amounts of their Private Information, including, on information and belief, their names, dates of birth, Social Security Numbers, medical information

---

[5] https://www.essehealth.com/about-us/our-story/ (last acc. May 16, 2025).
[6] https://www.essehealth.com/about-us/press-releases/esse-health-recognized-as-a-2019-top-150-privately-held-company/ (last acc. May 16, 2025).
[7] *Id.*
[8] *Id.*

such as diagnoses and treatment history, health insurance information, and payment information.

17. Esse collects and stores this Private Information on its information technology computer systems, on information and belief located at Defendant's headquarters in St. Louis, Missouri.

18. Defendant acknowledges the importance of protecting and securing the Private Information/PHI it collects.

19. For example, Esse Health states on its website in its Privacy Policy that: "Information about Users that is maintained on Esse Health's systems is protected using industry standard security measures."[9]

20. In addition, Esse represented to its patients that it will undertake adequate measures to safeguard their Private Information.

21. Esse Health also maintains a Notice of Privacy Practices ("Notice of Privacy Practices"), in which Esse Health acknowledges: "We are required by law to maintain the privacy and security of your protected health information. • We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information. • We must follow the duties and privacy practices described in this notice and give you a copy of it. • We will not use or share your information other than as described here unless you tell us we can in writing."[10]

22. In the Notice of Privacy Practices, Esse provides enumerated purposes for which it may disclose health information/Private Information, *inter alia*: for treatment, payment, and health care operations purposes. *See* **Exhibit C**, pages 3-4.

23. None of the enumerated purposes for which Defendant may disclose PHI/Private

[9] https://www.essehealth.com/privacy-policy/ (last acc. May 16, 2025) (attached as **Exhibit B**).
[10] *Esse Health Notice of Privacy Practices*, avail. at https://www.essehealth.com/wp-content/uploads/2019/05/Notice-of-Privacy-Practices.pdf (last acc. May 16, 2025) (**attached as Exhibit C).**

Information without authorization includes the Data Breach that came to pass due to Defendant's tortious misconduct.

24. Despite the above promises, Defendant does not adequately safeguard patient health information, and does not follow industry standard practices in securing this data.

B. Defendant Fails to Safeguard Patients' Private Information

25. In late April 2025, Defendant suffered a ransomware cyberattack in which its patients' Private Information was unauthorizedly disclosed—the Data Breach.

26. According to Esse Health, as it posted to its website sometime in late April 2025 or early May 2025 in the *Network Updates*:

> We are writing today to advise you that some Esse Health network systems are currently offline due to a cybersecurity event. **Our offices remain open and we continue to serve patients.**
>
> We are making progress in restoring systems, though it is possible that you may encounter some delays as we use back-up processes. For the time being, if you need to reach us or need to schedule an appointment, you can contact us by:
>
> 1. Sending a text message to the main phone number for your doctor's office. This is the most efficient and effective way to reach us.
>
> 2. Sending a message via our patient portal.
>
> 3. Calling your doctor's office directly. Please note that our phones' capabilities are currently limited, so we ask for extra patience if there are delays in calls connecting.
>
> If you attempted to contact us in recent days but have yet to hear back, please contact us again using one of these methods.
>
> We apologize for the inconvenience and concern created by this situation. We are working with third-party specialists to securely restore all systems and investigate this situation. Please know that the confidentiality, privacy and security of information in our care is of utmost importance. If our investigation determines that the confidentiality of data related to any individuals was compromised, we will notify them directly.[11]

[11] *Network Update,* **Exhibit A.**

27. As of May 13, 2025, Esse's systems had not been fully restored. On May 13, 2025, Esse described its progress:

> We continue to work diligently to restore systems, and we are making good progress. We have now restored key information-sharing functions across our network, which will make it easier to fulfill new or previously scheduled appointments or procedures.
>
> Additionally, due to certain systems coming back online, we can schedule appointments further out than before. With that said, if you need to reach us or need to schedule an appointment, the best way to contact us is still by:
>
> 1. Sending a text message to the main phone number for your doctor's office.
> 2. Sending a message via our patient portal.
> 3. Calling your doctor's office directly.
>
> Please note that our phones' capabilities remain limited.[12]

28. Ultimately, in its Network Updates, Defendant has neither confirmed nor denied that patient's Private Information was impacted in the Data Breach, and has not sent formal notice to patients or other individuals impacted by the Data Breach.

29. Esse has obfuscated key details of the Data Breach, failing to disclose to affected patients whether or not their Private Information was unauthorizedly disclosed in the Data Breach; the identity of the ransomware cybercriminal; whether Defendant paid the ransom; whether the cybercriminals themselves have said that Esse's Private Information was taken; and other pertinent details necessary for affected patients to take appropriate measures to protect themselves from the Data Breach.

30. On information and belief, Plaintiff's and the proposed Class Members' Private Information was unauthorizedly disclosed to third-party cybercriminals in Defendant Data Breach in late April 2025, potentially including but not limited to their names, dates of birth, Social Security Numbers, medical information such as diagnoses and treatment history, health insurance

[12] *Id.*

information, and payment information.

31. This fact seems known to Esse, but not yet communicated to its affected patients. According to media outlets, "hundreds of patients have reported their healthcare has been placed on hold," and local media reports "point to a possible ransomware incident."[13]

32. Defendant conduct, by acts of commission or omission, caused the Data Breach, including: Esse's failures to implement best practices and comply with industry standards concerning computer system security to adequately safeguard Private Information, allowing Private Information to be accessed and stolen, by failing to implement security measures that could have prevented, mitigated, or timely detected the Data Breach, and by failing to adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems, resulting in the Data Breach.

33. On information and belief, based on the nature of the ransomware cyberattack, Plaintiff's and the Class Members' Private Information, unauthorizedly disclosed to third-party cybercriminals in the Data Breach, has now or will imminently be posted to the Dark Web for public viewing and use, in the public domain, and utilized for fraudulent and criminal misuse.

C. Plaintiff's Experience

34. Plaintiff is a current patient of Defendant having received medical treatment from Esse.

35. As a condition of receiving medical treatment and other services from Defendant, Plaintiff was required to provide her Private Information to Esse, including but not limited to her name, date of birth, Social Security Number, medical information such as diagnoses and treatment history, health insurance information, and payment information.

[13] https://healthexec.com/topics/health-it/cybersecurity/independent-provider-group-hit-cyberattack-delays-patient-care (last accessed May 16, 2025).

36. Plaintiff is very careful to guard the confidentiality of her Private Information, and never stores this information in an unsecure setting nor disseminates it publicly.

37. In entrusting her Private Information to Defendant as a condition of receiving medical care and other services from Esse, Plaintiff believed that Esse would adequately safeguard that information, including as set forth in Esse's Notice of Privacy Practices. Had Plaintiff known that Esse did not utilize reasonable data security measures, Plaintiff would not have entrusted her Private Information to Defendant

38. On information and belief, Plaintiff's Private Information was unauthorizedly disclosed to third-party cybercriminals in Defendant Data Breach in April 2025 caused by Esse's misconduct.

39. As a direct and proximate result of the Data Breach permitted to occur by Defendant, Plaintiff has suffered, and imminently will suffer, injury-in-fact and damages, including the unauthorized disclosure of the Private Information itself, which, on information and belief due to the nature of the cyberattack, has been or imminently will be posted on the dark web for sale and used for fraudulent and criminal purposes.

40. Moreover, the Data Breach, and Esse's post-breach response, have seriously affected Plaintiff's ability to receive necessary medical care and treatment, as Plaintiff has been unable to access her Esse electronic medical records, interrupting her regular care.

41. Furthermore, Plaintiff has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of her Private Information in the Data Breach, and the lack of knowledge as to what information was disclosed.

42. In addition, as a result of the Data Breach, Plaintiff has been required and will be required to expend considerable time and effort to monitor her accounts and credit files to protect

himself from identity theft and fraudulent misuse of her Private Information disclosed in the Data Breach.

43. Had Plaintiff known that Defendant did not adequately protect her Private Information, she would not have entrusted her sensitive that data to Esse.

44. Plaintiff's sensitive Private Information remains in Defendant's possession in its computer systems without adequate protection against known threats, exposing Plaintiff to future breaches and additional harm.

45. As a result of Esse's Data Breach, its victims face a lifetime risk of identity theft, and increased risk of harm.

D. This Data Breach was Foreseeable by Defendant.

61. Plaintiff and the proposed Class Members provided their Private Information to Esse for the purpose of receiving medical treatment and with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

62. By failing to do so, Defendant put all Class Members at risk of identity theft, financial fraud, and other harms.

63. Defendant tortiously failed to take the necessary precautions required to safeguard and protect the Private Information of Plaintiff and the Class Members from unauthorized disclosure. Defendant actions represent a flagrant disregard of Plaintiff's and the other Class Members' rights.

64. Plaintiff and Class Members were the foreseeable and probable victims of Defendant inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of

providing adequate security for that information.

65. According to a Chief Strategy Officer at Clear DATA, "[i]t's no secret that healthcare is the industry most plagued by data breaches. Patient data is the most valuable, making it targeted by bad actors."[14]

66. Moreover, healthcare companies are targeted because of their cybersecurity vulnerabilities: "…healthcare is also targeted because it is very vulnerable. Many healthcare providers use outdated IT infrastructure and operating systems that can no longer be patched or supported, such as Windows 7 and Windows Server 2008, even after Microsoft retired them. Further, more than half of medical devices operate on legacy systems, and 83% of medical imaging devices are on outdated operating systems that no longer receive patches/updates. This creates significant cybersecurity vulnerabilities and makes it much easier for bad actors to find an entry point into the network." [15]

67. Cyber-attacks against healthcare organizations, such Defendant are targeted and frequent. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across U.S. healthcare organizations. Significant security incidents are a near-universal experience in U.S. healthcare organizations with many of the incidents initiated by bad actors…"[16]

68. In 2019, a record 1,473 data breaches occurred, resulting in approximately

---

[14] Sanjay Cherian, Forbes Magazine, "Healthcare Data: The Perfect Storm," January 14, 2022, available at https://www.forbes.com/sites/forbestechcouncil/2022/01/14/healthcare-data-the-perfect-storm/?sh=28523ee56c88 (last acc. June 19, 2023).

[15] *Id*.

[16] HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, *2019 HIMSS Cybersecurity Survey*, available at https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last accessed December 7, 2022)

164,683,455 sensitive records being exposed, a 17% increase from 2018.[17]

69. Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[18]

70. According to the Identity Theft Resource Center's January 24, 2022 report for 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[19]

71. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant industry, including Esse. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[20]

72. Furthermore, Defendant was aware of the risk of data breaches because such breaches have dominated the headlines in recent years. For instance, the 525 reported medical or healthcare data breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[21]

73. According to the U.S. Department for Health and Human Services' "2022

---

[17] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Dec. 7, 2022)
[18] *Ibid.*
[19] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last acc. Apr. 14, 2023).
[20] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last acc. Apr. 14, 2023).
[21] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Dec. 7, 2022), at pg. 15.

Healthcare Cybersecurity Year in Review, and a 2023 Look-Ahead," "[h]ealthcare data breaches have doubled in 3 years."[22]

74. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant industry, including Esse.

75. Private Information is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used for a variety of unlawful and nefarious purposes, including ransomware and fraudulent misuse, and sale on the Dark Web,

76. Private Information can be used to distinguish, identify, or trace an individual's identity, such as their names, Social Security numbers, and medical records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

77. Given the nature of the Data Breach, it was foreseeable that the compromised Private Information could be used by cybercriminals in a variety of different injurious ways. Indeed, the cybercriminals who possess the Plaintiff's and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in their names.

E. Defendant Fails to Comply with Industry Standards

78. As shown above, experts studying cyber security routinely identify organizations holding PII/PHI as being particularly vulnerable to cyber-attacks because of the value of the information they collect and maintain.

79. A number of industry and national best practices have been published and are

[22] U.S. Department for Health and Human Services, The Health Sector Cybersecurity Coordination Center (HC3), "2022 Healthcare Cybersecurity Year in Review, and a 2023 Look-Ahead," February 9, 2023, avail. at https://www.hhs.gov/sites/default/files/2022-retrospective-and-2023-look-ahead.pdf

widely used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security's (CIS) CIS Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including 18 Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[23]

80. In addition, the National Institute of Standards and Technology (NIST) recommends certain practices to safeguard systems, *infra,* such as:

a. Controlling who logs on to your network and uses your computers and other devices;

b. Using security software to protect data;

c. Encrypting sensitive data, at rest and in transit;

d. Conducting regular backups of data;

e. Updating security software regularly, automating those updates if possible;

f. Having formal policies for safely disposing of electronic files and old devices;

g. Training everyone who uses your computers, devices, and network about

[23] *See* https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Apr. 14, 2023).

cybersecurity.[24]

81. Upon information and belief, Esse failed to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and other industry standards for protecting Plaintiff's and the proposed Class Members' Private Information, resulting in the Data Breach.

F. Defendant Failed to Comply with FTC Guidelines

82. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

83. In 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which establishes cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of Private Information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the

[24] Understanding The NIST Cybersecurity Framework, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last acc. Apr. 14, 2023).

system; and have a response plan ready in the event of a breach.[25]

84. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[26]

85. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

86. These FTC enforcement actions include actions against entities failing to safeguard PII/PHI such as Defendant *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

87. Defendant failed to properly implement basic data security practices widely known throughout the industry. Defendant failure to employ reasonable and appropriate measures to protect against unauthorized access to patient Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

---

[25] *See* Federal Trade Commission, October 2016, "Protecting Private information: A Guide for Business," available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last acc. Apr. 14, 2023).

[26] *See id*.

88. Defendant was at all times fully aware of its obligations to protect the Private Information of Esse's patients that was entrusted to Esse. Defendant was also aware of the significant repercussions that would result from its failure to do so.

G. Defendant Conduct Violates HIPAA and Evidences Their Insufficient Data Security

89. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

90. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of sensitive patient health information. Safeguards must include physical, technical, and administrative components.

91. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. § 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information, like the data Defendant left unguarded. HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

92. The Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

93. Defendant breached its obligations to Plaintiff and the Class Members and/or were otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems, network, and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to adequately protect patients' Private Information;

b. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

c. Failing to practice the principle of least-privilege and maintain credential hygiene;

d. Failing to avoid the use of domain-wide, admin-level service accounts;

e. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords;

f. Failing to ensure the confidentiality and integrity of electronic PHI/ Private Information it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI/ Private Information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI/ Private Information that are not permitted under the privacy rules regarding individually identifiable health information in violation of

45 C.F.R. § 164.306(a)(3); and/or

k. Failing to render the electronic PHI/ Private Information they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI/ Private Information as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key," 45 CFR § 164.304 (definition of encryption);

94. As a result of its violations, Defendant negligently and unlawfully failed to safeguard Plaintiff's and the Class Members' Private Information.

H. Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

95. Cyberattacks in the healthcare industry are especially problematic because of the disruption they cause to the health treatment and overall daily lives of patients affected by the attack.

96. For instance, loss of access to patient histories, charts, images, and other information forces providers to limit or cancel patient treatment due to a disruption of service.

97. This is exactly what happened in this case, with the Data Breach that Esse permitted to occur not only making unavailable Esse's electronic health records system, MyChart, telephone systems, and "various systems utilized to order certain tests, procedures and medications" but actually preventing the Plaintiff and Class Members from accessing Defendant medical care.

98. Such disruptions lead to a deterioration in the quality of overall care patients receive at facilities affected by data breaches. This is an especially acute problem, because it is not as if incarcerated Class Members have any choice in who provides them care.

99. Researchers have found medical facilities that experience a data security incident incur an increase in the death rate among patients months and years after the attack.[27]

100. Researchers have further found that at medical facilities that experience a data security incident, the incident leads to a deterioration in patient outcomes, generally.[28]

101. Similarly, data security incidents inconvenience patients; these inconveniences include, but are not limited, to the following:

a. rescheduling of medical treatment;

b. being forced to find alternative medical care and treatment;

c. delays or outright cancellation of medical care and treatment;

d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

e. the indefinite loss of personal medical history.[29]

102. Cyber-attacks that result in the removal of protected data are also considered a breach under HIPAA as there is an access of PHI not permitted under the HIPAA Privacy Rule:

103. A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." 45 C.F.R. § 164.40.

104. Data Breaches like this represent a significant problem for patients who have

---

[27] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019) https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last accessed June 7, 2022).

[28] *See Data Breach Remediation Efforts and Their Implications for Hospital Quality*, Health Services Research https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last accessed June 7, 2022).

[29] *See, e.g.*, https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/ (last accessed September 1, 2021); https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech (last accessed on September 1, 2021).

already experienced the inconvenience and disruption associated with a cyber-attack.

I. The Data Breach Caused Plaintiff and the Class Members Injury and Damages

105. Plaintiff and Class Members have suffered injury and damages from the unauthorized disclosure and misuse of their Private Information that can be directly traced to Defendant that has occurred, is ongoing, and/or will imminently occur.

106. As stated prior, on information and belief, in the Data Breach, unauthorized cybercriminals were able to access the Plaintiff's and the proposed Class Members' Private Information, which is now being used or will imminently be used for fraudulent purposes and/or has been sold for such purposes and posted on the Dark Web for sale, causing widespread injury and damages.

107. The ramifications of Defendant failure to keep Plaintiff's and the Class's Private Information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes.

108. Because Defendant failed to prevent the Data Breach, Plaintiff and the proposed Class Members have suffered, will imminently suffer, and will continue to suffer injury-in-fact and damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the Class Members have suffered, and will imminently suffer:

a. Disruption of medical care;

b. The loss of the opportunity to control how Private Information is used;

c. Unauthorized use of stolen Private Information;

d. Emotional distress;

e. The compromise and continuing publication of their Private Information;

f. Out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

g. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

h. The diminution in value of their Private Information;

i. Delay in receipt of tax refund monies; and,

j. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Esse fails to undertake the appropriate measures to protect the Private Information in its possession.

109. Furthermore, the Data Breach has placed Plaintiff and the proposed Class Members at an increased risk of fraud and identity theft.

110. There are myriad dangers which affect victims of identity theft, including: cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and

fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.[30]

111. The FTC recommends that identity theft victims take several costly steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, seeking a credit freeze, and correcting their credit reports.[31]

112. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

113. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

114. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's Private Information to police during an arrest—resulting in an arrest warrant being issued in the victim's name. That can be even more problematic and difficult to remedy for someone who already has a criminal record.

115. Further, according to the Identity Theft Resource Center's 2021 Consumer

[30] *See* Gaetano DiNardi, Aura.com, "How Bad Is Identity Theft? Is It Serious?" (December 14, 2022) available at https://www.aura.com/learn/dangers-of-identity-theft#:~:text=Fraudsters%20can%20open%20new%20accounts,to%20repair%20your%20credit%20score (last acc. Feb. 27, 2023).
[31] *See* https://www.identitytheft.gov/Steps (last visited September 1, 2021).

Aftermath Report, identity theft victims suffer "staggering" emotional tolls: "For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. Thirty-three percent reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their mortgage. Fifty-four percent reported feelings of being violated." [32]

116. What's more, theft of PHI is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected through the lens of massively complex cloud computing, Private Information/PHI is a valuable property right.[33]

117. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that Private Information has considerable market value.

118. Theft of PHI, in particular, is problematic because: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[34]

---

[32] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (June 11, 2021), avail. at https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/ citing Identity Theft Resource Center, "2021 Consumer Aftermath Report," May 26, 2021 available at https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/ (last acc. Feb. 27, 2023).

[33] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private information") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[34] *See Medical Identity Theft, Federal Trade Commission Consumer Information* (last visited: June 7, 2022), http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

119. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

120. It must also be noted there may be a substantial time lag–measured in years–between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

121. PHI and PII are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

122. Where the most Private Information belonging to Plaintiff and Class Members was accessible from Defendant network, there is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and the Class Members are at an increased risk of fraud and identity theft for many years into the future.

123. Thus, Plaintiff and the Class Members must vigilantly monitor their financial and medical accounts for many years to come.

124. According to cybersecurity experts, "[r]eports show the value of a health record can be worth as much as $1,000, whereas on the dark web, a credit card number is worth $5 and Social Security numbers are worth $1."[35]

[35] Sanjay Cherian, Forbes Magazine, "Healthcare Data: The Perfect Storm," January 14, 2022, available at https://www.forbes.com/sites/forbestechcouncil/2022/01/14/healthcare-data-the-perfect-storm/?sh=28523ee56c88 (last acc. June 19, 2023).

125. Social Security numbers are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.[36]

126. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[37] Each of these fraudulent activities is difficult to detect. An individual may not know that her or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

127. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[38]

128. This data, as one would expect, demands a much higher price on the black market.

---

[36] *See* U.S. Social Security Administration, "Identity Theft and Your Social Security Number," Publication No. 05-10064, July 2021, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last acc. Feb. 25, 2023)

[37] *See id.*

[38] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited September 1, 2021).

Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[39] Medical information is especially valuable to identity thieves. The asking price on the Dark Web for medical data is $50 per person and up.[40]

129. Accordingly, the Data Breach has caused Plaintiff and the proposed Class Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein, specifically the imminent identity fraud and criminal fraudulent activity, fraudulent charges, theft of monies, and attendant costs; lost time and efforts in remediating the impact of the Data Breach, and other injury and damages as set forth in the preceding paragraphs.

130. Defendant knew or should have known of these harms which would be caused by the Data Breach it permitted to occur, and strengthened its data systems accordingly.

CLASS ACTION ALLEGATIONS

131. Pursuant to Missouri Court Rule of Civil Procedure 52.08, Plaintiff brings this class action individually, and on behalf of the following proposed Class (the "Class"):

> **All Missouri citizens whose Private Information was disclosed, accessed, or compromised in the Data Breach experienced by Defendant beginning in April 2025 as announced by Esse.**

132. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant's members, partners, subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which

---

[39] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited September 1, 2021).

[40] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last accessed September 1, 2021).

Defendant or their parents has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

133. The Class defined above is identifiable through Defendant's business records.

134. Plaintiff reserves the right to amend the class definition.

135. Plaintiff and the Class Members satisfy the numerosity, commonality, typicality, adequacy, and predominance prerequisites for suing as representative parties pursuant to Rule 52.08(a).

136. **Numerosity:** The exact number of Class Members is unknown but is estimated to be into the thousands of persons at this time, and individual joinder in this case is impracticable. Class Members can be easily identified through Defendant records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies.

137. **Typicality:** Plaintiff's claims are typical of the claims of other Class Members in that Plaintiff, and the Class Members sustained damages arising out of Defendant's Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiff and the Class Members sustained similar injuries and damages, as a result of Defendant's uniform illegal conduct.

138. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class actions to

vigorously prosecute this action on behalf of the Class. Plaintiff has no interests that conflict with, or are antagonistic to those of, the Class, and Defendant has no defenses unique to Plaintiff.

139. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

a. whether Defendant violated the laws asserted herein, and other statutory privacy and consumer protection laws;

b. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Private Information;

c. whether Defendant breached the duty to use reasonable care to safeguard Plaintiff's and the Class's Private Information;

d. Whether Defendant breached its contractual promises to safeguard Plaintiff's and the Class's Private Information;

e. whether Defendant was negligent *per se* in not complying with privacy laws;

f. whether Defendant knew or should have known its practices and representations related to the Data Breach, and Private Information were deceptive and unfair;

g. whether Defendant knew or should have known about the inadequacies of its data security policies and system and the dangers associated with storing sensitive Private Information;

h. whether Defendant failed to use reasonable care and industry standard,

reasonable methods to safeguard and protect Plaintiff's and the other Class Members' Private Information from unauthorized release and disclosure;

i. whether the proper data security measures, policies, procedures and protocols were in place and operational within Defendant's computer and software systems to safeguard and protect Plaintiff's and the other Class Members' Private Information from unauthorized release and disclosure;

j. whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

k. whether Defendant's delay in informing Plaintiff and the Class of the Data Breach was unreasonable;

l. whether Defendant's method of informing Plaintiff and the Class of the Data Breach was unreasonable;

m. whether Defendant's conduct was deceptive, unfair, or unconscionable, or constituted unfair competition;

n. whether Defendant's conduct was likely to deceive the public;

o. whether Defendant is liable for negligence or gross negligence;

p. whether Defendant's conduct, practices, statements, and representations about the Data Breach of the Private Information violated applicable state laws;

q. whether Defendant knew or should have known its representations were false, deceptive, unfair, and misleading;

r. whether Plaintiff and the Class were injured as a direct and proximate result of the Data Breach;

s. what the proper measure of damages is; and

t. whether Plaintiff and the Class Members are entitled to compensatory damages, and restitutionary, injunctive, declaratory, or other relief.

140. **Superiority**: This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Petition. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort and expense will be fostered, and uniformity of decisions ensured.

141. A class action is therefore superior to individual litigation because:

a. the amount of damages available to an individual plaintiff is insufficient to make litigation addressing Defendant's conduct economically feasible in the absence of the class action procedural device;

b. individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system; and

c. the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

142. In addition to satisfying the prerequisites of Rule 52.08(a), Plaintiff satisfies the requirements for maintaining a class action under Rule 52.08(b) because:

a. the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Defendants;

b. the prosecution of separate actions by individual Class Members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and

c. Defendant has acted or refused to act on grounds that apply generally to the proposed Class, thereby making final injunctive relief or declaratory relief herein appropriate with respect to the proposed Class as a whole.

d. questions of law or fact common to the members of the class predominate over any questions affecting only individual members, and that a class action is superior to other available methods for the fair and efficient adjudication of the controversy.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

143. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

144. Plaintiff and the Class Members entrusted their Private Information to Esse as a condition of receiving medical care and other services.

145. Defendant owed to Plaintiff and Class Members a duty to exercise reasonable care in handling and using the Private Information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

146. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failures to collectively adequately safeguard their Private Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Private Information—just like in the Data Breach that ultimately came to pass.

147. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members's Private Information by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

148. Defendant owed to Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their Private Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

149. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant inadequate security protocols. Defendant actively sought and obtained Plaintiff's and Class Members's Private Information as a condition of providing medical treatment and other services to them.

150. The risk that unauthorized persons would attempt to gain access to the Private Information, and misuse it, was foreseeable. Given that Defendant holds vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendant databases containing the Private Information—whether by a sophisticated ransomware cyberattack or otherwise.

151. Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiff and Class Members and the importance of exercising reasonable care in handling it.

152. Defendant breached its duties by failing to exercise reasonable care in supervising its agents and in handling and securing the Private Information of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff's and Class Members' injuries, and are negligent.

153. Defendant is further breaching its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and Class Members' injuries-in-fact.

154. As a direct, proximate, and traceable result of Defendant's negligence, Plaintiff and the Class Members have suffered or will imminently suffer injury-in-fact and damages, including

but not limited to disruption of medical care; loss of the opportunity to control how Private Information is used; unauthorized use of stolen Private Information; emotional distress; compromise and continuing publication of their Private Information; out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud; Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; diminution in value of their Private Information; delay in receipt of tax refund monies; and, the continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Esse fails to undertake the appropriate measures to protect the Private Information in their possession.

155. As a direct and proximate result, Plaintiff and the Class are entitled to recover damages including actual and compensatory damages, nominal damages, and punitive damages, as permitted by law.

156. Further, Plaintiff and the Class are entitled to injunctive relief ordering Defendant to strengthen its data security systems, monitoring procedures, and data breach notification procedures to prevent additional unauthorized disclosure of the Private Information in Defendant's possession.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

157. Plaintiff incorporates the above Paragraphs as if fully set forth herein.

158. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

159. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, patients' Private Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duties to protect Plaintiff's and the Class Members' sensitive Private Information.

160. Further, under HIPAA, Defendant had the duty to implement safeguards to prevent the misuse of the information and ensure the confidentiality, integrity, and availability of PHI/Private Information.

161. Defendant violated its duties under Section 5 of the FTC Act, as well as HIPAA, by failing to use reasonable measures to protect Plaintiff's and the Class's Private Information and by not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Esse had collected, and stored, and the foreseeable consequences of a Data Breach, including, specifically, the immense damages that would result to its patients in the event of a breach, which ultimately came to pass.

162. The harm that has occurred is the type of harm the FTC Act and HIPAA are intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid

unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

163. Defendant had a duty to Plaintiff and the Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class's Private Information.

164. Defendant breached its duties to Plaintiff and Class Members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

165. Defendant's violations of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations, including HIPAA, constitutes negligence *per se*.

166. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and Class Members would not have been injured.

167. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that their Data Breach would cause Plaintiff and Class Members to suffer the foreseeable harms associated with the exposure of their Private Information.

168. Had Plaintiff and Class Members known that Defendant did not adequately protect their Private Information, Plaintiff and Class Members would not have entrusted Defendant with their Private Information.

169. As a direct, proximate, and traceable result of Defendant's negligence *per se*, Plaintiff and the Class Members have suffered or will imminently suffer injury-in-fact and damages, including but not limited to disruption of medical care; loss of the opportunity to control how Private Information is used; unauthorized use of stolen Private Information; emotional

distress; compromise and continuing publication of their Private Information; out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud; Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; diminution in value of their Private Information; delay in receipt of tax refund monies; and, the continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Esse fails to undertake the appropriate measures to protect the Private Information in its possession.

170. As a direct and proximate result, Plaintiff and the Class are entitled to recover damages including actual and compensatory damages, nominal damages, and punitive damages, as permitted by law.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

171. Plaintiff incorporates the above Paragraphs as if fully set forth herein.

172. Defendant offered to provide medical care and other services and data security to Plaintiff and the Class Members in exchange for payment and Private Information.

173. In turn, and through internal policies described in the preceding paragraphs, and other conduct and representations, Esse agreed it would not disclose the Private Information it collects to unauthorized persons and that it would safeguard patient Private Information.

174. Plaintiff and the Class Members accepted Esse's offer by providing Private Information to Defendant and paying money for medical treatment.

175. Implicit in the parties' agreement was that Esse would adequately safeguard the

Private Information of Plaintiff and the Class Members and would provide them with prompt and adequate notice of all unauthorized access and/or theft of their Private Information.

176. Plaintiff and the Class Members would not have entrusted their Private Information to Esse in the absence of such an agreement with Defendants.

177. Esse materially breached the contract(s) they each had entered into with Plaintiff and the Class Members by failing to safeguard their Private Information, and by failing to notify them promptly of the Data Breach that compromised such information.

178. Esse further breached the implied contracts with Plaintiff and the Class Members by:

a. Failing to properly safeguard and protect Plaintiff's and Class Members's Private Information;

b. Failing to comply with industry standards, as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to properly supervise its agents in possession of Private information;

d. Failing to ensure the confidentiality and integrity of electronic Private Information that Defendant created, received, maintained, and transmitted.

179. The damages sustained by Plaintiff and Class Members as described above were the direct and proximate result of Esse's material breaches of their agreement(s).

180. Plaintiff and the Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of Esse.

181. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in

connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

182. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes its conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

183. Esse failed to advise Plaintiff and Class Members of the Data Breach promptly and sufficiently.

184. In these and other ways, Esse violated its duties of good faith and fair dealing.

185. Plaintiff and the Class Members have sustained injury-in-fact and damages because of Esse's breaches of its agreements, including breaches thereof through violations of the covenants of good faith and fair dealing.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

186. Plaintiff incorporates the above Paragraphs as if fully set forth herein.

187. This claim is pleaded as the alternative to the breach of implied contract claim.

188. Plaintiff and the Class Members conferred a benefit upon Defendant in the form of Private Information provided to Defendant along with payment, as a condition of receiving medical care and other services.

189. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class Members.

190. As a result of Defendant conduct, Plaintiff and Class Members suffered actual

damages in an amount equal to the difference in value between the value of services with reasonable data privacy and security practices and procedures, and the services without unreasonable data privacy and security practices and procedures that they received.

191. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the proposed Class Members' monies paid and their Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the Class Members would not have provided their Private Information, nor paid Defendant had they known Defendant would not adequately protect their Private Information.

192. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of its misconduct and the Data Breach alleged herein.

COUNT V
INVASION OF PRIVACY—PUBLIC DISCLOSURE OF PRIVATE FACTS
(On Behalf of Plaintiff and the Class)

193. Plaintiff incorporates the above Paragraphs as if fully set forth herein.

194. Plaintiff and the Class Members took reasonable and appropriate steps to keep their Private Information confidential from the public.

195. Plaintiff's and the Class Members' efforts to safeguard their own Private Information were successful, as their Private Information was not known to the general public prior to the Data Breach.

196. Plaintiff and the Class Members had a legitimate expectation of privacy to their Private Information, entrusted to Esse solely for purpose of receiving medical care and other services, and were entitled to the protection of this information against disclosure to unauthorized third parties.

197. Defendant owed a duty to Esse's patients, including Plaintiff and the Class Members, to keep their Private Information confidential.

198. Plaintiff's and the Class Members' Private Information is not of legitimate concern to the public.

199. Defendant knew or should have known that Plaintiff's and Class Members' Private Information was private, confidential, and should not be disclosed.

200. Defendant publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiff and the Class by disclosing and exposing Plaintiff's and Class's Private Information to enough people that it is reasonably likely those facts will become known to the public at large, including without limitation on the dark web and elsewhere.

201. The unauthorized release of Private Information by Defendant in the Data Breach is particularly harmful and would be offensive to a reasonable person of ordinary sensibilities.

202. Defendant has extensive knowledge of its patients' medical conditions and Esse undertook to provide medical care for them, and therefore Defendant has a special relationship with Plaintiff and the Class and Defendant disclosure of Private Information is certain to embarrass them and offend their dignity. Defendant should appreciate that the cyber- criminals who stole the Private Information would further sell and disclose the Private Information as they are doing. That the original disclosure is devastating to the Plaintiff and the Class, even though it originally may have only been disclosed to one person or a limited number of cyber-criminals, does not render it any less a disclosure to the public-at-large.

203. Missouri Courts, and courts of other states, have recognized a cause of action for an invasion of privacy for over a century. *See, e.g., Sullivan v. Pulitzer Broad. Co.*, 709 S.W.2d

475, 477 (Mo. 1986) (citing *Munden v. Harris*, 153 Mo. App. 652, 134 S.W. 1076 (1911)).

204. Plaintiff's and the Class's Private Information was publicly disclosed by Defendant in the Data Breach with reckless disregard for the reasonable offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendant knew and know that Plaintiff's and Class's Private Information is not a matter of legitimate public concern.

205. As a direct and proximate result of Defendant conduct, Plaintiff and members of the Class have suffered tangible injury-in-fact and damages, including but not limited to disruption of medical care; loss of the opportunity to control how Private Information is used; unauthorized use of stolen Private Information; emotional distress; compromise and continuing publication of their Private Information; out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; diminution in value of their Private Information; delay in receipt of tax refund monies; and, the continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Esse fails to undertake the appropriate measures to protect the Private Information in their possession.

206. As a direct and proximate result, Plaintiff and the Class are entitled to recover damages including actual and compensatory damages, nominal damages, and punitive damages, as permitted by law.

COUNT VI
VIOLATION OF THE MISSOURI MERCHANDISING PRACTICES ACT,
Mo. Rev. Stat. § 407.010 *et seq.*
(On Behalf of Plaintiff and the Class)

207. Plaintiff incorporates the above Paragraphs as if fully set forth herein.

208. The Missouri Merchandising Practice Act (the "MMPA") prohibits false, fraudulent, or deceptive merchandising practices to protect both consumers and competitors by promoting fair competition in commercial markets for goods and services.

209. The MMPA prohibits the "act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice, or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce." Mo. Rev. Stat. § 407.020.

210. The MMPA defines "Merchandise" as "any objects, wares, goods, commodities, intangibles, real estate or services." Mo. Rev. Stat. § 407.010(4).

211. Plaintiff, individually and on behalf of the Class, is entitled to bring an action pursuant to Mo. Rev. Stat. § 407.025, which provides in relevant part that: (a) Any person who purchases or leases merchandise primarily for personal, family or household purposes and thereby suffers an ascertainable loss of money or property, real or personal, as a result of the use or employment by another person of a method, act or practice declared unlawful by section 407.20, may bring a private civil action in either the circuit court of the county in which the seller or lessor resides or in which the transaction complained of took place, to recover actual damages. The court may, in its discretion, award the prevailing party attorneys' fees, based on the amount of time reasonably expended, and may provide such equitable relief as it deems necessary or proper. Mo. Rev. Stat. § 407.025.

212. Defendant is a "person" within the meaning of the MMPA in that Defendant is a

domestic, for-profit corporation. Mo. Rev. Stat. § 407.010(5).

213. Plaintiff and Class Members are "persons" under the MMPA because they are natural persons and they used Defendant's services for personal, family, and/or household use.

214. The Missouri Attorney General has specified the settled meanings of certain terms used in the enforcement of the MMPA. Specifically, Mo. Code Regs. tit. 15, § 60-8.020, provides:

(1) Unfair practice is any practice which—

(A) Either—

1. Offends any public policy as it has been established by the Constitution, statutes, or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or

2. Is unethical, oppressive, or unscrupulous; and

(B) Presents a risk of, or causes, substantial injury to consumers.

215. Proof of deception, fraud, or misrepresentation is not required to prove unfair practices as used in section 407.020.1., RSMo. (*See Federal Trade Commission v. Sperry and Hutchinson Co.*, 405 U.S. 233, 92 S.Ct. 898, 31 L.Ed.2d 170 (1972); *Marshall v. Miller*, 302 N.C. 539, 276 S.E.2d 397 (N.C. 1981); *see also*, Restatement, Second, Contracts, sections 364 and 365.

216. Pursuant to the MMPA and Mo. Code Regs. Tit. 15, § 60- 8.020, Defendant's acts and omissions fall within the meaning of "unfair."

217. Defendant engaged in a "trade" or "commerce" within the meaning of the MMPA with regard to services which are supposed to keep Plaintiff's and the Class Members's Private Information safe and secure.

218. Defendant engaged in unlawful practices and deceptive conduct, which emanated from its Missouri headquarters, in violation of the MMPA by omitting and/or concealing material

facts related to the safety and security of Plaintiff's and the Class Members's Private Information. Defendant's unfair and unethical conduct of failing to secure Private Information and failing to disclose the Data Breach caused substantial injury to consumers in that the type of consumers' activities, including medical, insurance, and financial fraud and identity theft. The impacted consumers have been placed in an immediate and continuing risk of harm from fraud, identity theft, and related harm caused by the Data Breach.

219. Defendant conduct of failing to secure data required Plaintiff and the Class to undertake time-consuming, and often costly, efforts to mitigate the actual and potential harm caused by the Data Breach's exposure of their Private Information.

220. Defendant conduct of concealing, suppressing, or otherwise omitting material facts regarding the Data Breach was likely to mislead reasonable consumers under the circumstances, and thus constitutes an unfair and deceptive trade practice in violation of the MMPA.

221. By failing to secure sensitive data and failing to disclose and inform Plaintiff and Class Members about the Breach of Private Information, Defendant engaged in acts and practices that constitute unlawful practices in violation of the MMPA. Mo. Ann. Stat. §§ 407.010, *et seq.*

222. Defendant engaged in unlawful practices and deceptive conduct in the course of its business that violated the MMPA including misrepresentations and omissions related to the safety and security of Plaintiff's and the Class's Private Information. Mo. Rev. Stat. § 407.020.1.

223. As a direct and proximate result of these unfair and deceptive practices, Plaintiff and each Class member suffered actual harm in the form of money and/or property because the disclosure of their Private Information has value encompassing financial data and tangible money.

224. Defendant's unfair" acts and practices include:

a. by utilizing cheaper, ineffective security measures and diverting those funds

to its own profits, instead of providing a reasonable level of security that would have prevented the hacking incident;

b. failing to follow industry standard and the applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data;

c. failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that it could take appropriate steps to mitigate the potential for identity theft and other damages;

d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' personal information; and

e. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA.

225. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' personal information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the

security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' personal information, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA.

226. Defendant's misrepresentations and omissions were material to consumers and made in order to induce consumers' reliance regarding the safety and security of Private Information in order to obtain consumers' Private Information and purchase of medical products and/or services.

227. Defendant's deceptive practices misled Plaintiff and the Class and would cause a reasonable person to enter into transactions with Defendant that resulted in damages.

228. As such, Plaintiff and the Class seek: (1) to recover actual damages sustained; (2) to recover punitive damages; (3) to recover reasonable attorneys' fees and costs; and (4) such equity relief as the Court deems necessary or proper to protect Plaintiff and the members of the Class from Defendant deceptive conduct and any other statutorily available damages or relief the court deems proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, MARY WIPPOLD, individually, and on behalf of all others

similarly situated, requests that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding Plaintiff and the Class damages that include applicable compensatory, actual, exemplary, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

E. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: May 20, 2025

Respectfully submitted,

/s/ John F. Garvey
John F. Garvey #35879
Colleen Garvey #72809
Ellen A. Thomas, #73043
STRANCH, JENNINGS & GARVEY, PLLC
701 Market Street
Peabody Plaza, Suite 1510
St. Louis, Missouri 63101
(314) 390-6750
jgarvey@stranchlaw.com
cgarvey@stranchlaw.com
ethomas@stranchlaw.com

Lynn A. Toops (Pro Hac Vice forthcoming)
Amina Thomas (Pro Hac Vice forthcoming)
COHENMALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
Telephone: (317) 636-6481
Facsimile: (317) 636-2593
ltoops@cohenmalad.com
athomas@cohenmalad.com

Counsel for Plaintiff and the Proposed Class

Certificate of Filing

The undersigned hereby certifies that the foregoing Class Action Petition has been filed by using the Court's electronic case filing system on this 20th day of May, 2025.

/s/ John F. Garvey

2522-CC00957

In the
CIRCUIT COURT
City of St. Louis, Missouri

For File Stamp Only

Mary Wippold, individually and on behalf of all others
Plaintiff/Petitioner

vs.

American Multispecialty Group, Inc., d/b/a Esse Hea
Defendant/Respondent

5/19/2025
Date

Case number

Division

REQUEST FOR APPOINTMENT OF PROCESS SERVER

Comes now Plaintiff (Requesting Party), pursuant to Local Rule 14, requests the appointment by the Circuit Clerk of

Name of Process Server	Address	Telephone
H&H Investigations, LLC	432 Hazelgreen, St. Louis, MO 63119	314-225-8114

to serve the summons and petition in this cause on the below named parties.

SERVE:
American Multispecialty Group, Inc., d/b/a Esse H
Name
12655 Olive Blvd., 4th Floor
Address
St. Louis, MO 63141
City/State/Zip

SERVE:
Name
Address
City/State/Zip

SERVE:
Name
Address
City/State/Zip

SERVE:
Name
Address
City/State/Zip

Appointed as requested:
TOM KLOEPPINGER, Circuit Clerk

By_____
Deputy Clerk

Date

John F. Garvey
Attorney/Plaintiff/Petitioner
35879
Bar No.
701 Market St., Ste. 1510, St. Louis, MO 63101
Address
(314) 390-6750
Phone No.

RULE 14 SPECIAL PROCESS SERVERS

1. Any person appointed by the Court or the Circuit Clerk to serve process must have a license issued pursuant to this rule to serve process.

2. Licenses to serve process shall be issued by the Sheriff of the City of St. Louis if the applicant has met the following qualifications:

   a. Is twenty-one years of age or older;

   b. Has a high school diploma or an equivalent level of education;

   c. Has insurance coverage for any errors or omissions occurring in the service of process;

   d. Has not been convicted, pleaded guilty to or been found guilty of any felony, or of any misdemeanor involving moral turpitude; and,

   e. Has passed a training course for the service of process which shall be administered by the Sheriff of the City of St. Louis.

3. Each applicant for a process server license under the provisions of this rule shall provide an affidavit setting forth such person's legal name, current address, any other occupations and current telephone numbers. Licensed process servers shall immediately notify the Sheriff of the City of St. Louis of any change in the above information, and the failure to do so shall constitute good cause for the revocation of such person's license.

4. The Sheriff of the City of St. Louis shall maintain a list of persons licensed to serve process pursuant to this rule, and shall make such list available to litigants upon request.

5. A photo identification card designed by the Sheriff of the City of St. Louis shall be issued in addition to the license. No other identification will be allowed. All licenses must be signed and approved by the Sheriff of the City of St. Louis and the Presiding Judge or his designee.

6. A license fee recommended by the Sheriff and approved by the Court En Banc shall be charged to cover the costs of compiling and maintaining the list of process servers and for the training of such process servers. The license fees shall be made payable to the Sheriff of the City of St. Louis.

7. A license for service of process issued under this rule may be revoked by the Sheriff with the approval of the Presiding Judge or his designee, for any of the following reasons:

   a. Misrepresentation of duty or authority;

   b. Conviction, guilty plea or finding of guilty of any state or federal felony, or a misdemeanor involving moral turpitude;

   c. Improper use of the license;

   d. Making a false return; or

   e. Any other good cause.

   Provided, no service of process made by an appointed process server with a revoked license shall be void if the Court or Circuit Clerk made the appointment in good faith without knowledge of the license revocation.

8. Any person authorized to serve process may carry a concealed firearm as allowed by Section 506.145, RSMo, only while actually engaged in the service of process and only if the person has passed a firearms qualification test approved by a law enforcement agency; provided, however, that any licensed special process server may file a written waiver of the right to carry a concealed firearm and thereby avoid the requirements of firearm training and testing. Any violation of this section shall be considered beyond the scope of the privilege to carry a concealed weapon that is granted by the appointment, and shall constitute good cause for the revocation of the license.

9. Applications for the appointment of a special process server shall be made on forms available in the offices of the Sheriff and Circuit Clerk. Orders Appointing special process servers may list more than one licensed server as alternatives.

10. The licenses granted pursuant to this rule shall be good for two years. Each person granted a license shall be required to reapply at the expiration of the license and shall be required to provide all the information required in the initial application, including a current police record check.

(Approved 9/28/92; amended 11/23/92; 5/31/95; 12/17/07)

Summons in Civil Case

IN THE 22ND JUDICIAL CIRCUIT, CITY OF ST LOUIS, MISSOURI

Judge or Division: CHRISTOPHER EDWARD MCGRAUGH	**Case Number: 2522-CC00957**	
Plaintiff/Petitioner: MARY WIPPOLD vs.	Plaintiff's/Petitioner's Attorney/Address JOHN FRANCIS GARVEY JR 701 MARKET ST SUITE 1510 ST LOUIS, MO 63101	
Defendant/Respondent: AMERICAN MULTISPECIALTY GROUP INC	Court Address: CIVIL COURTS BUILDING 10 N TUCKER BLVD SAINT LOUIS, MO 63101	(Date File Stamp for Return)
Nature of Suit: CC Breach of Contract		

The State of Missouri to: AMERICAN MULTISPECIALTY GROUP INC
Alias: D/B/A ESSE HEALTH

12655 OLIVE BOULEVARD
FOURTH FLOOR
SAINT LOUIS, MO 63141

SPECIAL PROCESS SERVER

You are summoned to appear before this court and to file your pleading to the petition, a copy of which is attached, and to serve a copy of your pleading upon the attorney for plaintiff/petitioner at the above address all within 30 days after receiving this summons, exclusive of the day of service. If you fail to file your pleading, judgment by default may be taken against you for the relief demanded in the petition.

COURT SEAL OF

CITY OF ST LOUIS

May 23, 2025
Date

Clerk

Further Information:

Case Number: 2522-CC00957

Officer's or Server's Return

Note to serving officer: Service should be returned to the court within 30 days after the date of issue.

I certify that I have served the above Summons by: (check one)

☐ delivering a copy of the summons and petition to the defendant/respondent.

☐ leaving a copy of the summons and petition at the dwelling house or usual place of abode of the defendant/respondent with _____, a person at least 18 years of age residing therein.

☐ (for service on a corporation) delivering a copy of the summons and petition to: _____ (name) _____ (title).

☐ other: _____.

Served at _____ (address) in _____ (County/City of St. Louis), MO, on _____ (date) at _____ (time).

_____ Printed Name of Officer or Server

_____ Signature of Officer or Server

Must be sworn before a notary public if not served by an authorized officer.
Subscribed and sworn to before me on _____ (date).

(Seal)

My commission expires: _____ Date _____ Notary Public

Service Fees (if applicable)

Summons	$_____
Non Est	$_____
Sheriff's Deputy Salary	
Supplemental Surcharge	$ 10.00
Mileage	$_____ (_____ miles @ $._____ per mile)
Total	**$**_____

A copy of the summons and petition must be served on **each** defendant/respondent. For methods of service on all classes of suits, see Supreme Court Rule 54.

Summons in Civil Case

IN THE 22ND JUDICIAL CIRCUIT, CITY OF ST LOUIS, MISSOURI

Judge or Division: CHRISTOPHER EDWARD MCGRAUGH	**Case Number: 2522-CC00957**
Plaintiff/Petitioner: MARY WIPPOLD vs.	Plaintiff's/Petitioner's Attorney/Address JOHN FRANCIS GARVEY JR 701 MARKET ST SUITE 1510 ST LOUIS, MO 63101
Defendant/Respondent: AMERICAN MULTISPECIALTY GROUP INC	Court Address: CIVIL COURTS BUILDING 10 N TUCKER BLVD SAINT LOUIS, MO 63101
Nature of Suit: CC Breach of Contract	(Date File Stamp for Return)

The State of Missouri to: **AMERICAN MULTISPECIALTY GROUP INC**
Alias: D/B/A ESSE HEALTH

12655 OLIVE BOULEVARD
FOURTH FLOOR
SAINT LOUIS, MO 63141

SPECIAL PROCESS SERVER

You are summoned to appear before this court and to file your pleading to the petition, a copy of which is attached, and to serve a copy of your pleading upon the attorney for plaintiff/petitioner at the above address all within 30 days after receiving this summons, exclusive of the day of service. If you fail to file your pleading, judgment by default may be taken against you for the relief demanded in the petition.

COURT SEAL OF

CITY OF ST LOUIS

May 23, 2025
Date

Clerk

Further Information:

Case Number: 2522-CC00957

Officer's or Server's Return

Note to serving officer: Service should be returned to the court within 30 days after the date of issue.

I certify that I have served the above Summons by: (check one)

☐ delivering a copy of the summons and petition to the defendant/respondent.

☐ leaving a copy of the summons and petition at the dwelling house or usual place of abode of the defendant/respondent with _____, a person at least 18 years of age residing therein.

☒ (for service on a corporation) delivering a copy of the summons and petition to: Daphne Foster (name) Admin to CA (title).

☐ other: _____.

Served at 12655 Olive Blvd St. Louis, Mo 63141 (address) in St. Louis (County/City of St. Louis), MO, on 5/28/25 (date) at 1:45 pm (time).

Joseph Dolan Specin Process Serv #722
Printed Name of Officer or Server

SPS #722
Signature of Officer or Server

Must be sworn before a notary public if not served by an authorized officer.
Subscribed and sworn to before me on _____ (date).

(Seal)

My commission expires: _____ _____
Date Notary Public

Service Fees (if applicable)

Summons	$_____
Non Est	$_____
Sheriff's Deputy Salary	
Supplemental Surcharge	$ 10.00
Mileage	$_____ (_____ miles @ $._____ per mile)
Total	$_____

A copy of the summons and petition must be served on **each** defendant/respondent. For methods of service on all classes of suits, see Supreme Court Rule 54.